NATO OTAN
Science & Technology Organization (STO)

Protecting GNSS Critical Infrastructure in an Unstable World

Francisco Gallardo López,[1,2] Antonio Pérez Yuste,[1] David Sánchez Heredero[2]
[1]Universidad Politécnica de Madrid
ETSI Sistemas de Telecomunicación
C/ Nikola Tesla s/n, 28031, Madrid
SPAIN

[2]DLR GfR mbH
GERMANY

francisco.gallardo@dlr-gfr.com

ABSTRACT

In the current geopolitical situation, the disruption and falsification of GNSS (Global Navigation Satellite Systems) signals poses a severe threat for the defence operations of the European Union (EU) and NATO, and puts civil operations, like airlines and maritime operators, in danger. Several areas in the world are experiencing this problem in almost a continuous manner over the last few months (e.g., East border of the EU and Middle East, among others).

This paper discusses the work performed by the Universidad Politécnica de Madrid (UPM) and DLR GfR mbH in the field of detection and protection of attacks to GNSS signals for critical infrastructure, developing technologies that were applied in ESA (European Space Agency) projects like RESIST, for worldwide detection of GNSS Spoofers and Jammers. This paper will discuss the results of the application of the AI-based developed systems CMCU (Central Machine Learning Unit) and RESIST to different fields and projects. A brief discussion on new techniques developed on top of these two is outlined.

RESUME

Dans la situation géopolitique actuelle, la perturbation et la falsification des signaux GNSS (Systèmes Mondiaux de Navigation par Satellite) représentent une menace grave pour les opérations de défense de l'UE et de l'OTAN, et mettent en danger les opérations civiles telles que celles des compagnies aériennes et des opérateurs maritimes. Plusieurs régions du monde sont confrontées à ce problème de manière quasi continue au cours des derniers mois (par exemple, la frontière orientale de l'UE et le Moyen-Orient, entre autres).

Cet article présente les travaux réalisés par l'Université Polytechnique de Madrid (UPM) et DLR GfR mbH dans le domaine de la détection et de la protection contre les attaques visant les signaux GNSS pour les Infrastructures Critiques (IC), en développant des technologies appliquées dans des projets de l'ESA (Agence Spatiale Européenne) tels que RESIST, pour la détection mondiale des brouilleurs et des usurpateurs de signaux GNSS. Cet article expose les résultats de l'application des systèmes développés à base d'intelligence artificielle, CMCU (Unité Centrale d'Apprentissage Automatique) et RESIST, dans différents domaines et projets. Une brève discussion sur les nouvelles techniques développées à partir de ces deux systèmes est également présentée.

KEYWORDS

Global Navigation Satellite Systems (GNSS); Jamming; Low Earth Orbit (LEO); Machine Learning; Satellites; Spoofing.

1.0 CURRENT CHALLENGES RELATED TO THE GLOBAL NAVIGATION SATELLITE SYSTEMS ACROSS CRITICAL INFRASTRUCTURE: NAVWAR

GNSS (Global Navigation Satellite Systems) jamming and spoofing pose a severe threat across key sectors, as GNSS is widely used across many applications, including critical infrastructure. Due to the current geopolitical tensions, the navigation and timing service provided by GNSS (e.g., Galileo, GPS, Glonass, etc.) have been targeted.

With the aim of either disrupting the services or forcing wrong information into the victim's navigation systems, two main types of attacks have been recently put in place at a massive scale: GNSS jamming and GNSS spoofing.

This type of incidents has been recently referred to as "NAVWAR" (Navigation Warfare) [1], considered as a subset of the wider Electronic Warfare (EW) concept.

The following sections showcase how this type of incidents impact several markets.

Aviation

These types of incidents are impacting the aviation sector, potentially compromising the accuracy and reliability of navigation systems. This leads to navigation errors, increases risk of mid-air collisions, and causes disruptions in air traffic management [2]. Additionally, GNSS vulnerabilities in aviation systems can result in delayed flights, increased fuel consumption due to inefficient routing, and potential safety hazards during take-off and landing. Some evidence collected in the literature is referred to below.

Figuet et al., in Ref. [2], revealed that GNSS jamming incidents have led to considerable air traffic disruptions in Eastern Europe. The study highlighted that, during a jamming event, there was a significant increase in the number of aircraft deviating from their planned routes, leading to a 15% rise in fuel consumption and a 20-minutes average delay per flight.

Nováka et al., in Ref. [3], provided concrete evidence of dangers posed by GNSS interference during critical phases of flight. Their investigation demonstrated that GNSS interference could severely impact the precision of instrument approaches, with potential deviations of up to 30 metres from the intended glide path. This deviation not only increases the risk of runway excursions but also compromises the overall safety of the landing process.

Tegler, in Ref. [4], revealed that these incidents are continuously observed in the Baltic region of Europe. In those cases, it leads to a manual disabling of the GPS navigation systems when flying through the regions of northern and Baltic Europe to prevent contamination of other navigation systems (i.e., inertial, etc.). Figure 1 provides a clear snapshot of how intentional radio frequency interferences represent a serious hazard to aviation due to the adverse impact on air traffic and on the security of people.

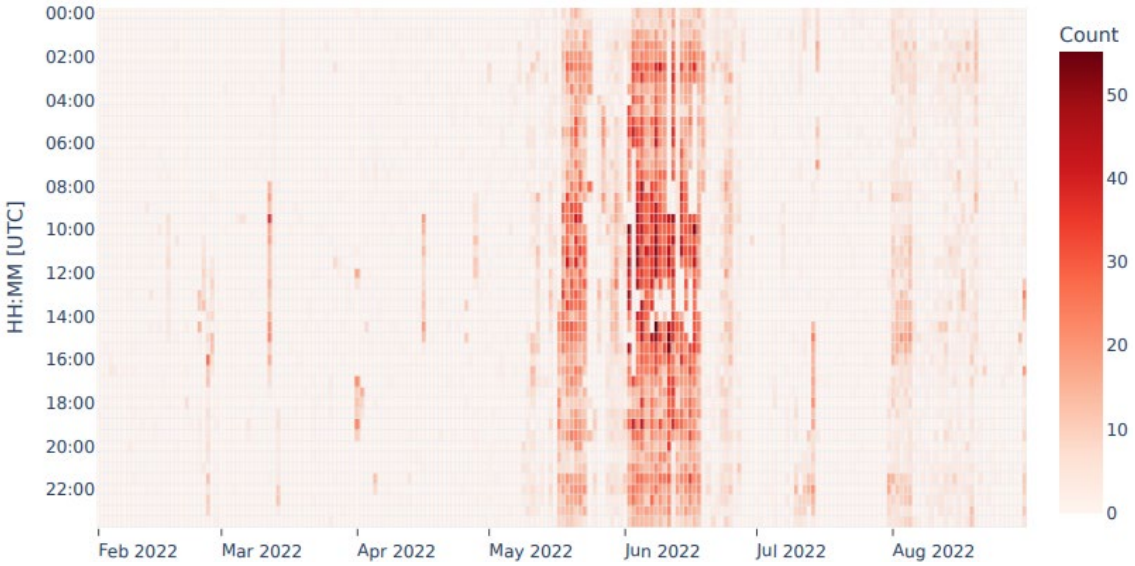

Figure 1: Number of flights influenced by RFI (Radio Frequency Interference) activities per 30-min interval over the entire observation period (22 hours), in Eastern Europe. The colour varies as a function of the number of flights affected by RFI for the corresponding 30-min interval [2].

Maritime

In the maritime sector, GNSS vulnerabilities can lead to significant navigational errors, posing substantial risks to vessel safety and maritime traffic management. According to the study by Grant et al., in Ref. [5], these vulnerabilities can have pronounced impacts on the sector. One major consequence of GNSS disruption is the misinformation transmitted by the Automatic Identification System (AIS), causing Vessel Traffic Services/Management (VTS) to receive incorrect data, thereby compromising the accuracy of their situational awareness.

Furthermore, the reliability of Differential Global Positioning System (DGPS) services and Aids to Navigation (AtoNs) could be severely affected, rendering the provided information unreliable. Onboard ships, these vulnerabilities can lead to failures in the Digital Selective Calling (DSC) emergency communication system, eliminating the ability to accurately report their location in emergencies.

For example, Medina et al., in Ref. [6], provide with a deeper understanding of the implied technical challenges. This study reports experiments conducted in the Baltic Sea, illustrating the extent of GNSS jamming threats in maritime navigation.

Additionally, Liu et al., in Ref. [7] highlight specific examples of severe impacts of GNSS spoofing. The research found that during spoofing attacks, vessels experienced positional deviations, leading to potential collisions and grounding. Moreover, the integrated navigation systems onboard were unable to differentiate between authentic and spoofed signals, exacerbating navigational errors and endangering vessel safety.

In this market, the most reknowned event was the GNSS spoofing situation that took place in 2019 in Shanghai [8]. As shown in Figure 2, vessels were reporting wrong positions and velocities around a particular building at the riverside. This kind of phenomenon is referred to as “circle spoofing.”

Figure 2: AIS data capture. As can be seen, due to GNSS spoofing, a large number of vessels reported sailing over ground, around a specific point [8].

Defence

The defence sector heavily relies on GNSS for various applications, including navigation, targeting, and communications. Jamming and spoofing attacks on GNSS can compromise military operations by disrupting these critical services. For example, during a NATO exercise in 2018, GNSS jamming affected military operations in Northern Europe, leading to significant disruptions in navigation and communication systems for various military units. This incident, reported by both Defence News and Inside GNSS, underscored the vulnerability of military operations to GNSS interference, with Norway and Finland noting significant signal disruptions attributed to Russian military activities [9], [10], [11].

Another notable example arises from the conflict in Syria, where GNSS jamming and spoofing has been widely reported. In 2019, Israeli defence forces reported that GNSS spoofing originating from Syria affected both military and civilian aircraft, causing them to receive incorrect positional data. This has been part of ongoing electronic warfare in the region, demonstrating the strategic impact of GNSS vulnerabilities [12], [13].

Other Sectors

Other sectors, such as infrastructure and emergency services, also face risks from GNSS jamming and spoofing. For instance, GPS jamming can affect critical infrastructure, including power grids and telecommunications networks, leading to widespread disruptions. In particular, the impact of GNSS jamming to timing services, like the ones required for 5G, is well known [14]. The same can also be expected from spoofing. Note that timing could also be a targeted service, having a severe impact across a variety of industries, as IT systems widely rely on timing services for secure communications, licensing of core process tools, etc. For example, mobile communication systems and data networks use GNSS time to keep all base stations in perfect synchronization and to coordinate handover operations between them [15]. It is worth noting that the International Telecommunication Union (ITU) does not refer to GNSS spoofing as a thread in [15], only jamming is mentioned, making a standardization framework for spoofing detection an urgent need. In 2017, a jamming incident in Norway disrupted GPS signals over a large area, affecting aviation, maritime, and emergency services. This event highlighted the potential for GNSS interference to impact multiple sectors simultaneously [14], [15].

Emergency services relying on GNSS for rapid response times can experience delays, potentially endangering lives. Events like those in 2019 in Shanghai [8], may impact emergency response vehicles that could be delayed due to incorrect routing information, underlining the potential impact on lifesaving operations. Additionally, financial systems that depend on precise timing from GNSS signals can be compromised, leading to transaction errors and security breaches. A notable incident in 2017 involved a European financial institution that experienced timing discrepancies due to GNSS jamming, causing significant transaction errors and operational delays [16].

These real-world cases illustrate the broad and severe impacts of GNSS jamming and spoofing across various sectors, emphasizing the need for comprehensive measures to protect and secure GNSS-dependent systems.

1.1 GNSS Jamming

GNSS jamming is a form of Denial of Service attack that involves deliberately transmitting signals to disrupt a receiver's access to Positioning, Navigation and Time (PNT) services, and disrupting its capability to compute Position Velocity and Time (PVT). This definition of jamming [16] implies that the generation of a GNSS waveform, with no Navigation Message [17] would also be considered to be a jamming attack. GNSS signals are especially vulnerable to jamming because they are very weak when reaching the surface of Earth, which makes overpowering genuine satellite navigation signals quite straightforward and achievable with low size, weight and power devices.

Waveforms generated for this purpose typically consist of Continuous Wave (CW), Chirp signals, Gaussian Noise, or even GNSS-like waveforms (see above). Such signals need to be transmitted in the same bandwidth used for the nominal provision of the satellite navigation services. It should again be noted that this definition focuses on the attacker's goal, rather than the waveform itself: either with a DoS (jamming attack) or causing the victim compute an incorrect PNT (spoofing attack).

It should be noted that jamming attacks are sometimes performed prior to the start of a spoofing attack [18] to "blind" the victim's receiver tracking loops in advance, which makes the subsequent spoofing attack not immediately evident.

1.2 GNSS Spoofing

This type of attack is more complex than the jamming attack. In this case, the attacker generates waveforms and data like those generated by real GNSS satellites. This type of attack is possible by means of three options: either causing the victim to estimate wrong pseudo-ranges to faked satellites, generating fake navigation messages, or both options together.

Should the attacker generate a completely fake navigation message with a GNSS-like signal, a simple GNSS laboratory-grade single-purpose signal generator or an SW GNSS signal generator (currently available for free on the Internet) with standard COTS (Commercial-off-the-Shelf) SDR (Software Defined Radio) HW (HardWare), would be more than enough to perpetrate an attack.

In some cases, an attacker may need to use the authentic navigation message to avoid detection—such as when constrained by the use of Galileo's Open Service Navigation Message Authentication (OS-NMA), which provides cryptographic protection of the navigation message. Such protection adds a way for end-users to check the authenticity of the navigation message, which makes some parts of the navigation message unpredictable for spoofing attacks). In this case, only the attack vector will be based on generating fake signals, using the real navigation messages (i.e., the attack will be solely based on making the victim compute fake pseudo-ranges). This type of attack is called Secure Code Estimation and Replay (SCER) [19], and requires a real time estimation of the unpredictable symbols transmitted by the satellites or the usage of directive antennas and isolated channels per satellite, adding the delays and Dopplers as needed, to make the victim to compute

wrong pseudo-ranges. Clearly, this makes the SCER attack more complex but, at the same time, the only remaining resort for the attackers since Galileo OS-NMA will be widely adopted by the GNSS user community.

Other details to consider include the capacity of the attacker to align fake signals with real ones, from the victim's receiver point of view (spoofing synchronous attack), which makes detecting the beginning of an attack more difficult. Should the attacker not be able to (or not be interested in) aligning the fake signal with the real one at the receiver's Antenna Phase Centre (APC), the attack will not be synchronous. Needless to say, aligning the signals in the victim's APC is a complex task and requires *a priori* knowledge of the victim's location, as well as an adequate real time estimation of motion. Consequently, by combining both considerations, the most complex attack to detect would be a Synchronous SCER attack.

1.3 Future GNSS Supporting Solutions

GNSS providers (e.g., GPS and Galileo), are planning the next steps to enhance security for the GNSS OS (Open Service) user community. To that end, services like the Galileo OS-NMA (Open Service Navigation Message Authentication) are being deployed, along with future services that will involve including unpredictability elements at higher frequencies in the signals(i.e., SCA [Spread Code Authentication]). GPS is indeed planning the deployment of a system called Chimera (Chips-Message Robust Authentication), which will combine both SCA and NMA [20]. Clearly, it is highly likely that Galileo will also include such SCA capabilities in the future.

The reason for adopting NMA capabilities in the GNSS OS is to prevent spoofing attacks that don't use the real navigation message. By including some time dependency in the keys that are used (as in the case of the Galileo TESLA OS-NMA protocol), the attacker is forced to estimate symbols on-the-fly when trying to overcome the unpredictability of the NMA symbols. Such SCER attacks, use a combination of matched filters and Bayesian estimators to determine the value of the transmitted symbols. Every symbol value is the mathematical expectation of the output of a matched filter [18]. Thus, by using the nomenclature from [19] for Galileo E1B in Base Band (BB), the output when the spoofer uses a full local copy of the E1B signal can be expressed as:

$$E\left[Z_{l_{E_{full}}}(n)\right] = W_L + 1 - E\left[\frac{9}{11}[W_L + 1]\varepsilon(n)\right] \quad (1)$$

Where:

$$\varepsilon(n) = \frac{1}{n}\sum_{k=K_l}^{K_l+n-1} e_{1_{C_k}} e_{1_{B_k}} \quad (2)$$

W_L is an NMA symbol that the spoofer needs to estimate in advance to be included it in its fake signal, "n" is the number of samples used for the integration in the receiver's matched filter, "k" is the length of the Galileo E1 Pseudo Random Noise (PRN) employed for spreading the spectrum of the transmitted signal, and $Z_{l_{E_{full}}}(n)$ is the output of the matched filter, when the attacker is using a full Galileo E1 signal as local copy in its own receiver. Finally, in Eq. (2), $e_{1_{C_k}} e_{1_{B_k}}$ is the product of the E1C and E1B PRNs of the Galileo satellite being used for the symbol estimation.

Rather than forcing the attacker to estimate a transmitted symbol, if the attacker needs to estimate the chip value of the PRN sequence, then the window for the estimation is greatly reduced (4092 times in the case of Galileo E1B). Such change makes the SCER harder to be perform, although it does not render the attack impossible, as the attacker may still try to use separate channels and directive antennas to avoid the need of estimating the symbol in real time. Such setup is, of course, more complex for the attacker [19].

The expectation of the matched filter the attacker will face, should SCA be used, will be (assuming the local copy used by the attacker includes a known symbol and the full subcarrier of Galileo E1B+C) [19]:

$$E\left[Z_{l_{E_{partialSCA}}}(n)\right] = e_{1B_k} - E\left[\frac{9}{11}\varepsilon_{SCA}(n)\right] \quad (3)$$

where:

$$\varepsilon_{SCA}(n) = \frac{1}{n}\sum_{k=K_l}^{K_l+n-1} e_{1_{C_k}} w_k \quad (4)$$

Note that in this case, the goal is to estimate the value of the chip sign of the e_{1B_k} PRN. While the attacker had a maximum of 4 ms to estimate the NMA symbol, in the SCA case, the attacker has less than 1 µs to perform the estimation. The shorter the time available for the attacker to integrate samples in the matched filter, the lower the probability of accurately estimating the unpredictable symbol or chip.. This is why SCA is expected to become a key technology in the near future for protecting Open Service users against SCER attacks.

Note that Galileo signals were used in this example, but GPS signals will render similar results when their satellites start transmitting similar Binary Offset Carriers (BOC) signals and Open Service authentication services.

2.0 DETECTION SYSTEMS

As a result of the collaboration between the Technical University of Madrid (UPM) and DLR GfR mbH, several different systems were developed, with the aim of detecting GNSS jamming and spoofing. In the case of spoofing, these methods are complementary to the Galileo OS-NMA.

2.1 CMCU Operation Principles

The Central Machine Learning Computation Unit (CMCU) is based on the processing of raw signal Intermediate Frequency (IF) signals and applying Machine Learning (ML) to detect and quickly flag the presence of GNSS jamming and/or spoofing signals in a geographical area. RESIST, which includes the CMCU algorithm, is a natural extension of the original CMCU, which was only based on receiving antennas on the ground to feed the detection system.

2.2 CMCU

The CMCU, as described in Refs. [19] and [21], processes raw (Intermediate Frequency) IF signals recorded on the ground to extract a set of novel features that are then fed into ML algorithms, particularly decision trees and ADABoost (Adaptive Boosting).

The extracted features, the so-called Model-Gaussian Signal (MGS) feature extraction and the RFI presence, are at the CMCU core. The MGS process, together with a parallel RFI detection that works on the time domain by looking into signal energy increases, are key to properly feeding the ML models with meaningful data, both for training and detection. The core algorithm, including the MGS, can be seen in Figure 3.

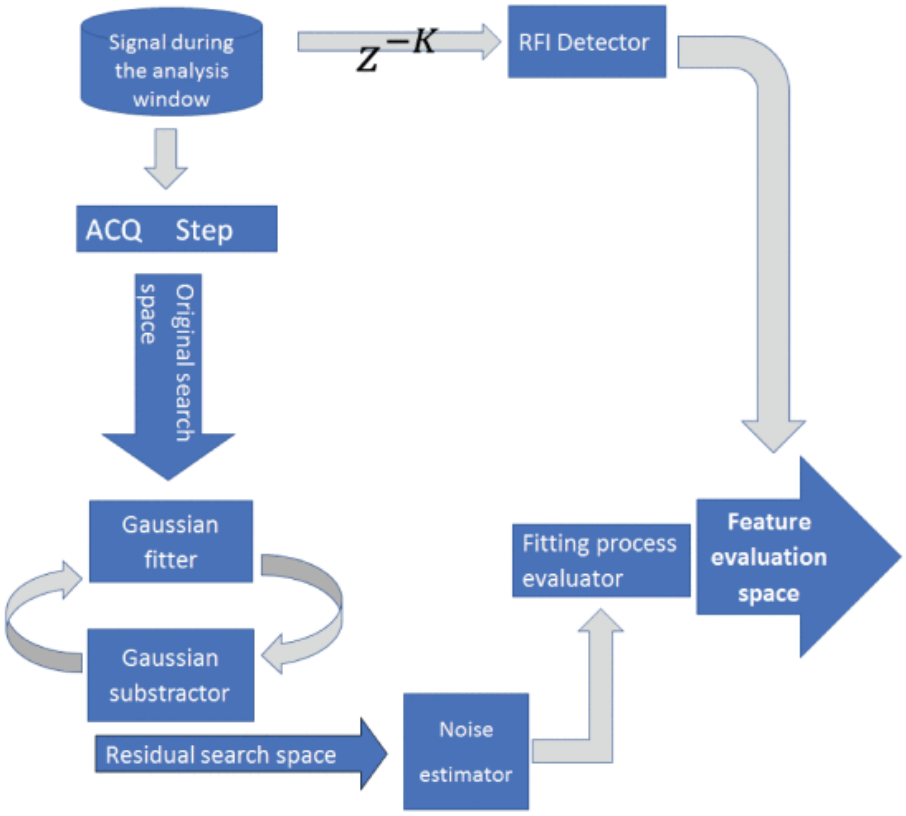

Figure 3: Core MGS extraction and RFI detector of CMCU algorithm [19].

In parallel to the RFI time domain, the GNSS search space is computed for each of the GNSS satellites. A bi-dimensional Gaussian fitting process is then conducted, subtracting the fitted Gaussian from the original search space. After the Gaussians have been subtracted, the remaining noise in the search space is estimated. All of these features (i.e., the Gaussian amplitudes and standard deviations, the remaining noise after the Gaussian subtraction, and the presence or absence of jamming signals) are fed to different Machine Learning models. More details can be found in Ref. [19].

The way in which CMCU integrates the MGS, RFI detection and ML prediction processes can be seen in Figure 4. The orchestrator launches one parallel process per GNSS satellite to be protected, and one extra process for the signal reception and distribution to each one of the channels. The signal consumer module gets the data from digitizers via a UDP (User Datagram Protocol) network socket. This ensures the CMCU can be deployed separately from the signal source (although the required bandwidth must be accounted for). The CMCU is deployed via docker containers, which helps with the CI/CD (Continuous Integration/Continuous Delivery) processes.

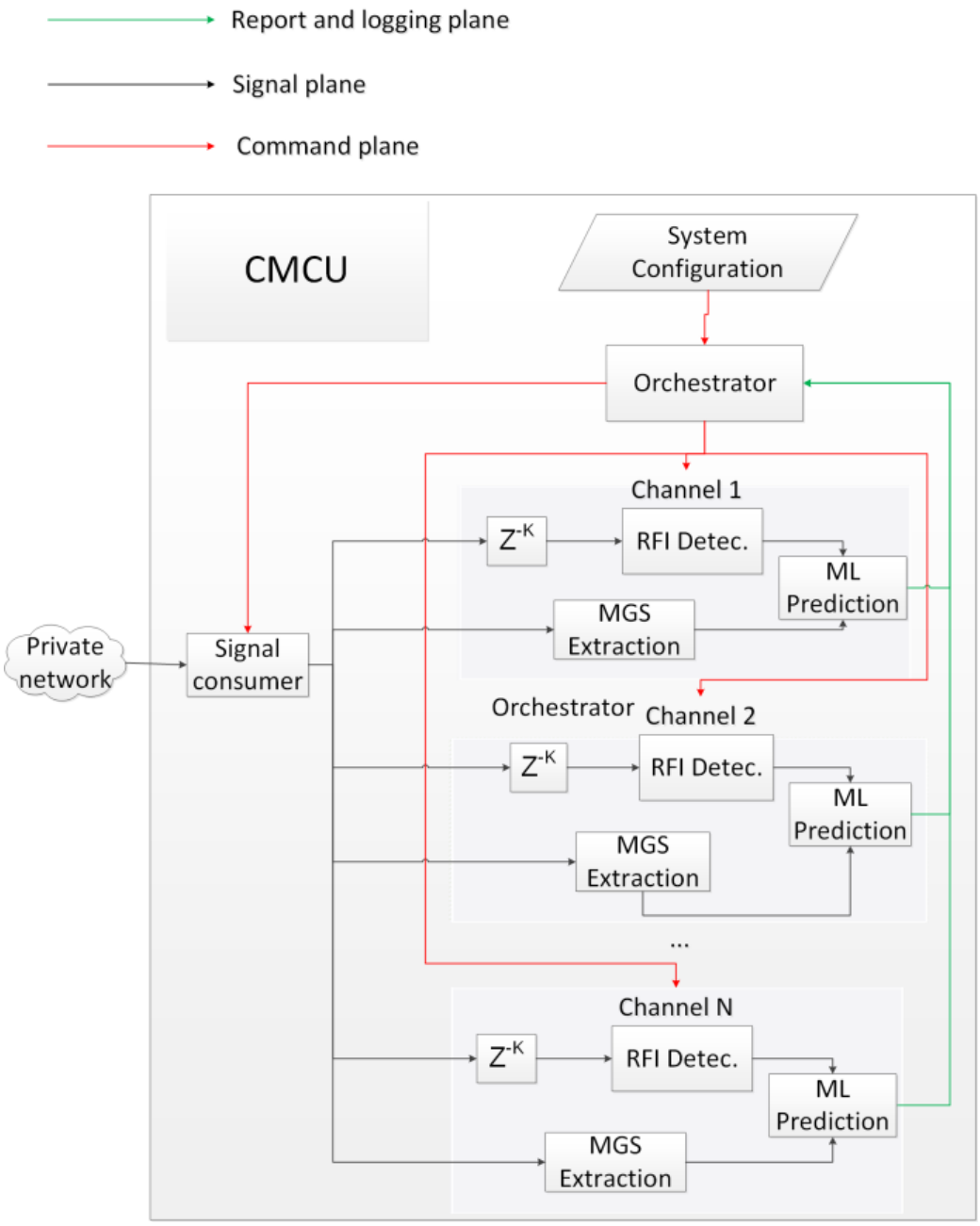

Figure 4: Operational CMCU algorithm internal structure [21].

Like any other operational system that relies on ML, CMCU requires the deployment of an additional environment, on top of the classically required ones (e.g., development environment, validation environment and operational environment), which is the ML training environment.

The CMCU suite instance deployed in such an environment has a special configuration (for ML training) that allows the network casting of predefined curated data (raw records of IF signal files). Such datasets are already labeled with the information regarding the presence of GNSS jamming and spoofing signals. In this configuration, the CMCU trains the ML algorithms with the data and the predefined information regarding the presence of the attacks.

As a result, the Training System generates a binary file with the trained model. This kind of model can be loaded into the operational environment of the CMCU, as a simple Configuration Item (CI). Reports about the expected performance (PMD and PFA) are also generated. In order to derive such information, the K-folds method is used [19]. The operator can configure the number of splits to be used (currently, however, a configuration of K = 5 and a distribution of 70% of data for training and 30% for validation is being used). See Figure 5 for more details.

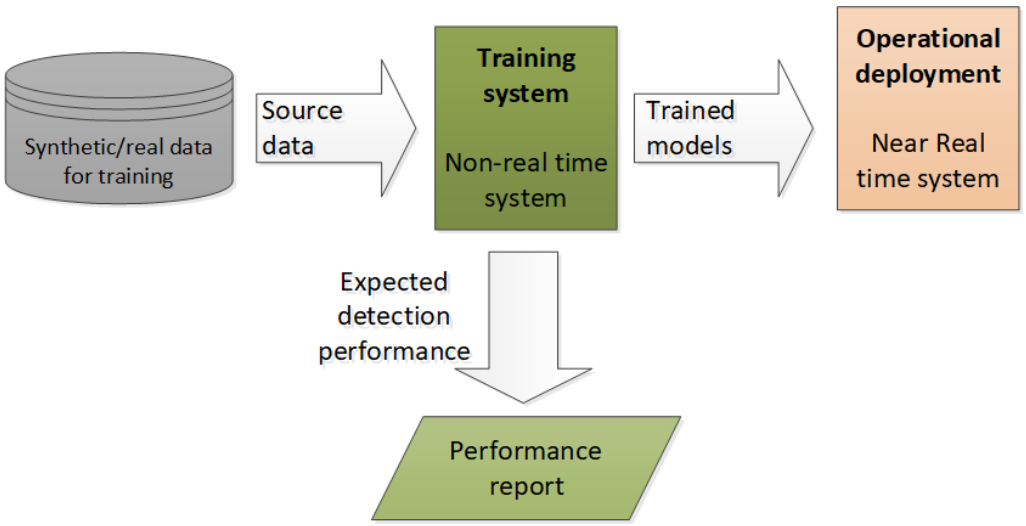

Figure 5: Relationship between operational and training systems for CMCU.

A setup like this allows the model to be updated in the operational platform in a very flexible way, as the training can be done without impacting service provision and the models can be tested in advance to avoid unexpected regressions.

Currently, the achieved performance for the Probability of Missed Detection is $PMD < 1e^{-6}$, and the achieved performance for the Probability of False Alarm, $PFA < 1e^{-6}$. The time of detection is approximately of 150 ms, running in non-real time operating systems. Further improvement in detection delay is expected in the near future by adding HW acceleration boards (e.g., GPUs or FPGAs).

Other solutions, like those referred in Ref. [22] and [23], base their detection methods on Neural Networks (NN). The method described in Ref. [22] demonstrates performance with a PMD $< 7e^{-3}$ and PFA $< 6e^{-3}$. The solution in [23] provides a PMD $< 8e^{-3}$ and PFA $< 2.6e^{-2}$. The authors of Ref. [24] base their proposed system on Deep Learning and inputs derived from Short-Time Fourier Transformations, providing a limited accuracy of 53.9%. The authors of Ref. [25] obtain an accuracy of 80% by feeding the GNSS search space into Neural Networks. The solution proposed in [26], using Multi-Layer Perception Neural Networks fed with GNSS tracking loop metrics and Automatic Gain Control (AGC) metrics, provides an accuracy of 89%. The authors of Ref. [27] fed Support Vector Machines (SVMs) with GNSS observables (Pseudo-ranges, Carrier phases, Carrier-to-noise ratios and Doppler shifts) using PCA (Principal Component Analysis) for dimensionality reduction, obtaining an accuracy of 98.72%.

Other proposed solutions, not based on ML algorithms, like the one provided in Ref. [28], obtain significant results of $PMD < 1e^{-3}$ and $PFA < 1e^{-3}$, as well as a time to alarm of 1 second.

Table 1: Comparison of CMCU results with the literature.

Reference	Features	Machine Learning Models	Accuracy
E. Shafiee et al. [22]	Early, prompt and late correlator outputs.	Multi-Layer Neural Network	99.37%
M. Riahi et al. [23]	Pseudoranges, Doppler shifts, carrier phase shift and carrier-to-noise ratios.	Neural Network	98.3%
C. Guo et al. [24]	IQ samples.	Convolutional Neural Network	65.6%
C. Guo et al. [24]	STFT	Deep Learning (RESNET50)	53.9%
P. Borhani-Darian et al. [25]	GNSS search space.	Multi-Layer Neural Networks	80%
S. Tohidi et al. [26]	GNSS tracking loop metrics, AGC metrics.	Multi-Layer Perceptron Neural Network (MLP NN)	89%
S. Semanjski [27]	GNSS observables (pseudorange, Carrier phase, signal-to-noise ratio and Doppler shifts). PCA is used for dimensionality reduction.	Support Vector Machine (SVM) classifiers	98.72%
M. Turner et al. [28]	High resolution GNSS search space is computed.	***Not based on AI/ML***: A maximum likelihood ratio test is used, to determine whether the PDF (Probability Density Function) matches the one in normal (non-spoofed) conditions	99.97%
This methodology (CMCU)	Model-Gaussian Signal (MGS) in the Search Space and parallel jamming time domain detection.	Decision Trees	99.9998%

2.3 RESIST

The RESIST system heavily relies on the CMCU and is a natural extension of its system concept. Thanks to a project funded by the European Space Agency (ESA) (IAP.FS.OT.003 RF Analytics Applications), RF analytical Evaluation of Signal In Space Threats (RESIST) was developed. The feasibility study aimed at providing a worldwide GNSS jamming and spoofing detection system based on injecting raw IF signals recorded by LEO (Low Earth Orbit) constellations into the CMCU. Two specific use cases were under study: service provision to maritime users/markets and service provision to companies that provide added value services based on GNSS (e.g., GNSS corrections services or the Global Navigation Satellite Systems themselves). Different workshops with key industry players were held to discuss the use cases and the system requirements. A system integrating the CMCU was designed, and a proof of concept was implemented, including a considerable amount of the system baseline requirements.

RESIST is about to enter its end-to-end testing phase, including testing in a maritime port in Spain and an airport in Germany. Several entities will act as end-users, including airports, airlines, companies using AIS data, and maritime ports.

RESIST combines the original CMCU concept of using ground-based IF signals with IF signals recorded from LEO constellations. This extends CMCU coverage, allowing the detection of jamming and spoofing incidents, without the need of having ground assets in place. A CMCU with a model trained solely with space data is deployed along the ground-based data trained models from the original CMCU, which allows the seamless combination of ground and space assets. See Figure 6 for the RESIST concept.

A key strength of RESIST is its seamless integration of both ground-based and space-based data. Space-based data is essential for monitoring regions where deploying ground antennas is not feasible. However, this approach has limitations — the revisit time of satellite constellations can restrict detection frequency, and only high-grade, military-level GNSS jamming and spoofing incidents are typically detectable from space. For continuous (24/7) protection or to detect low-power (faint) attacks, it is recommended to deploy a ground-based CMCU asset in the area that needs protection.

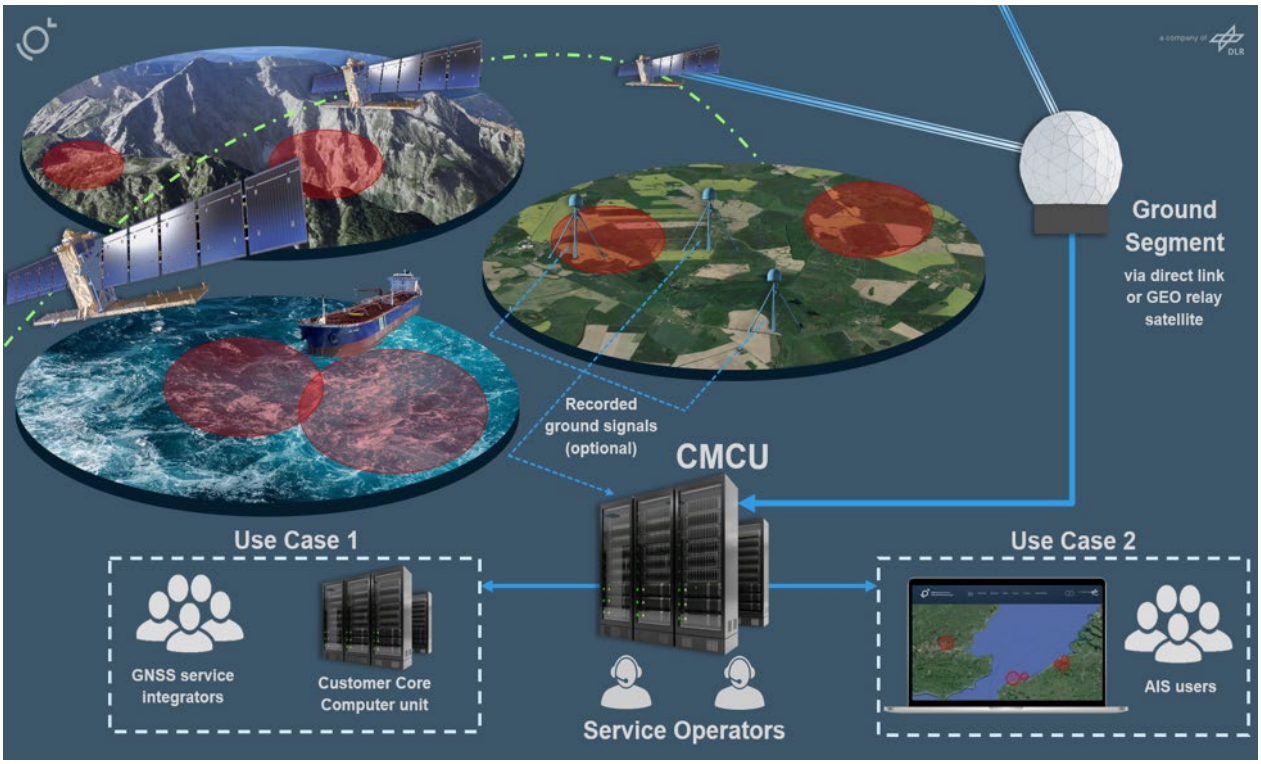

Figure 6: RESIST overall concept.

During the RESIST feasibility study, the Model-Based Systems Engineering (MBSE) Arcadia methodology was used for the system design. This methodology is a structured approach to identify and check the architecture of complex systems. The methodology fosters collaboration among all stakeholders throughout multiple engineering phases, using a shared system model across various levels. This collaborative approach was essential for effectively communicating the system design and requirements to users during the project. It also supports iterative development during the definition phase, enabling system architects to progressively refine the design and ensure all identified needs are met.

As a result of applying the Arcadia approach in the ESA feasibility study, a system design was proposed and implemented, having the CMCU in its core. The result can be seen in Figure 7. Various blocks of RESIST are described in the paragraphs that follow.

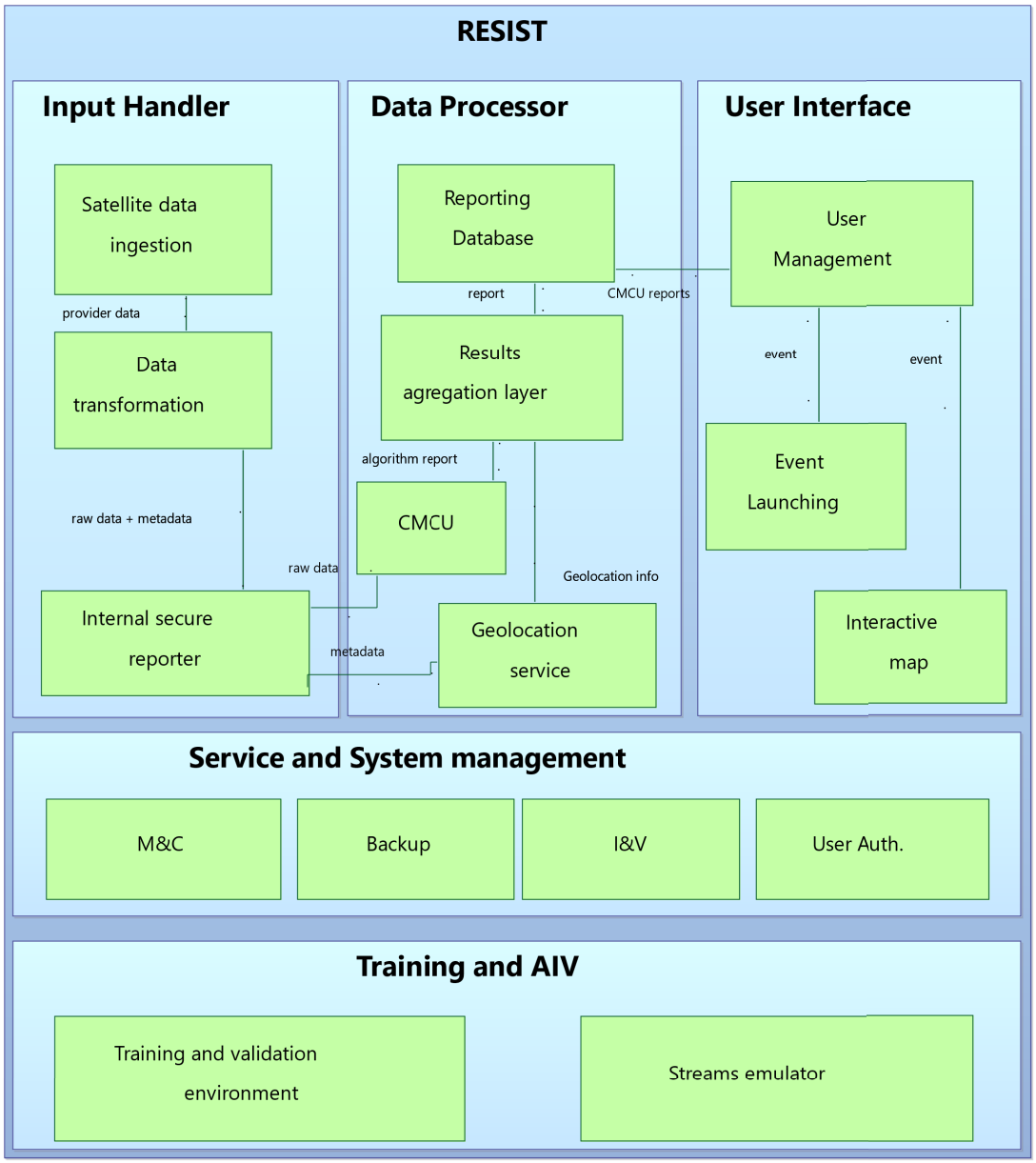

Figure 7: RESIST System design.

Input Handler

This block receives the raw data collected by the data provider. Signals are recorded from a LEO constellation and given to the core RF Analytics to be analysed. The input handler is composed of the satellite data ingestion functions, the Data Transformation function and the Internal secure reporter function.

Data Processor

This block evaluates the input data, and its processing is divided into two stages. First, the geographical information related to the recorded signals needs to be estimated. In parallel, the raw data is evaluated by the CMCU (the core algorithm of the system), which will analyse the presence of a jamming/spoofing attack and report the results in a database.

The internal blocks of this stage include the Geolocation service function, the CMCU, the Results aggregation layer and the Reporting database.

User Interface

Via the User Interface, the user has access to the RESIST core algorithm reports. The interface usage depends on the use case and the user's needs. The internal blocks are the User Management block, the Event Launcher (API), and the Interactive Map.

Service and Management System

This block includes all of the support and control functional blocks, grouping all of the functionalities related to the monitoring and control of the RESIST elements and required support functionalities, including: Backup management functions, Monitoring and control functions, Integration and Validation (I&V), and User Authentication capabilities.

Training and AIV (Assembly Integration and Validation)

The AIV functional blocks integrate the functionalities associated with the validation of the RF Analytics components and training of operators. The Streams emulator simulates the reception of LEO satellites data, with and without jamming and spoofing. This last item is based on the injection into the system of pre-recorded datasets which may be real or synthetic.

Performance with real signals will be assessed during the end-to-end testing phase of RESIST. As for performance based on simulated datasets, it is similar to the one obtained with the original CMCU. Note that the search space configuration is different, to compensate for the LEO dynamics, implying more computation load to the space model-based CMCU. This requires the use of computationally intensive processors (e.g., Intel(R) Xeon(R) Silver 4316 CPU or better). The RESIST component that tackles the ground recorded data has a CMCU performance of $PMD < 1e^{-6}$ and $PFA < 1e^{-6}$.

The same comparison between CMCU and the available literature that was highlighted in the CMCU section holds true for the ground assets. For the space assets (the LEO satellites), the comparison will be performed when the end-to-end testing phase is completed.

3.0 CONCLUSIONS

This paper showcases the work performed by UPM (Universidad Politécnica de Madrid) and DLR GfR mbH in developing several systems to protect critical infrastructure against GNSS jamming and spoofing.

An analysis of the current global situation and how these events impact the aviation, maritime and defence sectors has been provided, as well as an analysis on how the most complicated types of spoofing attacks (SCER attacks) are performed.

The operating principles and structure of the CMCU and RESIST systems were included, highlighting operational needs that such systems, based on Machine Learning, require. Performance of the current CMCU, as well as RESIST (with simulated datasets) have been provided.

Both solutions could provide complementary solutions to critical infrastructure users and providers, allowing them to know in advance that an area they are heading to may be experiencing a GNSS jamming or spoofing incident and react accordingly.

Future work will include the end-to-end testing of RESIST, assessing its performance with real signals.

4.0 REFERENCES

[1] Howell, D., "AFRL Navigation Warfare (NAVWAR) Testbed," in 22nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2009), Savannah, GA, 2009.

[2] Figuet, B., Waltert, M., Felux, M., and Olive, X, "GNSS Jamming and Its Effect on Air Traffic in Eastern Europe," Engineering Proceedings, vol. 28, no. 1, p. 12, 2022.

[3] Nováka, A., Jůn, F., Škultétya, F. and Novák Sedlačková, A. "Experiment Demonstrating the Possible Impact of GNSS Interference on Instrument Approach on RWY 06 LZZI," Transportation Research Procedia, vol. 43, no. 4, pp. 74-83, 2019.

[4] Tegler, E. "GPS Spoofing Is Now Affecting Airplanes in Parts of Europe," Forbes, 2024.

[5] Grant, A., Williams, P., Ward, N. and Basker, S. "GPS Jamming and the Impact on Maritime," The Journal of Navigation, vol. 62, no. 2, pp. 173-189, 2009.

[6] Medina, D. Lass, C., Pérez, E., Ziebold, R., Closas, P. and García, J. "On GNSS Jamming Threat from the Maritime Navigation Perspective," 22th International Conference on Information Fusion (FUSION). IEEE, pp. 1-7, 2019.

[7] Liu, Y., Li, S., Fu, Q., and Liu, Z., "Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System," Sensors, vol. 18, no. 5, p. 1433, 2018.

[8] Xiaojun, K.Z., "BACKGROUND: GNSS Spoofing in China and Beyond," Risk Intelligence A/S, 2021.

[9] O'Dwyer, G. "Finland, Norway Press Russia on Suspected GPS Jamming During NATO Drill," DefenseNews, 2018.

[10] Goff, S. "Russia Jammed GPS Signals During NATO Military Exercise Involving US Troops," Inside GNSS, 2018.

[11] Tanner, J. "Norway Says Russia Jammed GPS Signal During NATO Drill," C4SRNET, 2018.

[12] Divis, D. "New Report Details GNSS Spoofing Including Denial-of-Service Attacks," Inside GNSS, 2019.

[13] Batchelor, T. "Russia 'Deliberately Disrupted GPS Signals During NATO Drill'," Independent, 2018.

[14] Wührl, T., Baross, M.T., Gyáni, S. et al. "5G Synchronization Problems with GNSS Interference," IEEE 6th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE), pp. 000149-000154, 2023.

[15] International Telecommunication Union, "ITU-T G.8272.1 (01/2024)," ITU Publications, 2024.

[16] Borio, D. "GNSS Jammers: Effects and Countermeasures," in 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing, Noordwijk, 2012.

[17] C4ADS, "Above Us Only Stars," 2019.

[18] Humphreys, T.E., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073-1090, 2013.

[19] Gallardo, F. and Pérez, A. "SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection," IEEE Access, vol. 8, pp. 85515-85532, 2020.

[20] Motella, B. "Enhanced GNSS Authentication Based on the Joint CHIMERA/OSNMA Scheme," IEEE Access, vol. 9, pp. 121570-121582, 2021.

[21] Gallardo, F. and Pérez, A. "Operational Deployment of GNSS Anti-Spoofing System for Road Vehicles," Springer. Communication Technologies for Vehicles, pp. 50-60, 2021.

[22] Shafiee, E., Mosavi, M.R., and Moazedi,, M. "Detection of Spoofing Attack Using Machine Learning Based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," Journal of Navigation, pp. 169-188, 2018.

[23] Manesh, M.R, Kenney, J., Hu, W.C., et al. "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-6, 2019.

[24] Chengjun, G., and Yang, Z. "A Robust RF Fingerprint Extraction Scheme for GNSS Spoofing Detection," in Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023), Denver, Colorado, 2023.

[25] Borhani-Darian, P., Li, H., Wu, H., and Closas, P. "Deep Neural Network Approach to Detect GNSS Spoofing Attacks," Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), pp. 3241-3252, 2020.

[26] Tohidi, S. and Mosavi, M.R., "Effective Detection of GNSS Spoofing Attack Using a Multi-Layer Perceptron Neural Network Classifier Trained by PSO," 25th International Computer Conference, Computer Society of Iran (CSICC), pp. 1-5, 2020.

[27] Semanjski, S, Semanjski, I., De Wilde, W., and Gautama, S. "GNSS Spoofing Detection by Supervised Machine Learning with Validation on Real-World Meaconing and Spoofing Data-Part II," Sensors (Basel), 2020.

[28] Turner, M., Wimbush, S., Enneking, C., and Konovaltsev, A. "Spoofing Detection by Distortion of the Correlation Function," in IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, 2020.